



# **Norman Security Suite for Workstations**

**Version 7**

**User's Guide**

## **Limited warranty**

Norman guarantees that the enclosed CD-ROM and documentation do not have production flaws. If you report a flaw within 30 days of purchase, Norman will replace the defective CD-ROM and/or documentation at no charge. Proof of purchase must be enclosed with any claim.

This warranty is limited to replacement of the product. Norman is not liable for any other form of loss or damage arising from use of the software or documentation or from errors or deficiencies therein, including but not limited to loss of earnings.

With regard to defects or flaws in the CD-ROM or documentation, or this licensing agreement, this warranty supersedes any other warranties, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

In particular, and without the limitations imposed by the licensing agreement with regard to any special use or purpose, Norman will in no event be liable for loss of profits or other commercial damage including but not limited to incidental or consequential damages.

This warranty expires 30 days after purchase.

The information in this document as well as the functionality of the software is subject to change without notice. The software may be used in accordance with the terms of the license agreement. The purchaser may make one copy of the software for backup purposes. No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the explicit written permission of Norman.

The Norman logo is a registered trademark of Norman ASA.

Names of products mentioned in this documentation are either trademarks or registered trademarks of their respective owners. They are mentioned for identification purposes only.

Norman documentation and software are

Copyright © 1990-2007 Norman ASA.

All rights reserved.

Last revised on 13 December 2007.

---

## **Norman Offices**

### **Norman Data Defense Systems AS**

Blangstedgårdsvej 1, DK-Odense SØ, **Denmark**

Tel: +45 6311 0508 Fax: +45 6313 3901

email: normandk@normandk.com Web: <http://www.norman.no/dk>

### **Norman France**

8 Rue de Berri, 75008 Paris, **France**

Tel: +33 1 42 99 94 14 Fax: +33 01 42 99 95 01

email: info@norman.fr Web: <http://www.norman.fr>

### **Norman Data Defense Systems GmbH**

Zentrale, Gladbecker Str. 3, 40472 Düsseldorf, **Germany**

Tel.: +49 0211 / 5 86 99-0 Fax: 0211 / 5 86 99-150

email: info@norman.de Web: <http://www.norman.de>

### **Norman Data Defense Systems**

Centro Direzionale Lombardo, Via Roma, 108

20060 Cassina de' Pecchi (MI), **Italy**

Tel: +39 02 951 58 952 Fax: +39 02 951 38 270

email: info@normanit.com Web: <http://www.normanit.com>

### **Norman/SHARK BV**

Postbus 159, 2130 AD, Hoofddorp, **The Netherlands**.

Tel: +31 23 789 02 22 Fax: +31 23 561 3165

email: support@norman.nl Web: <http://www.norman.nl>

### **Norman ASA**

Mailing address: P.O. Box 43, N-1324, Lysaker, **Norway**.

Physical address: Strandveien 37, Lysaker, N-1324 Norway.

Tel: +47 67 10 97 00 Fax: +47 67 58 99 40

email: norman@norman.no Web: <http://www.norman.no/no>

### **Norman Data Defense Systems**

Camino Cerro de los Gamos 1, Edif.1

E - 28224 Pozuelo de Alarcón MADRID, **Spain**

Tel: +34 91 790 11 31 Fax +34 (0) 91 790 11 12

email: norman@normandata.es Web: <http://www.normandata.es>

### **Norman Data Defense Systems AB**

Korsgatan 2, 602 33 Norrköping, **Sweden**

Tel: +46 11 - 230 330 Fax: +46 11 - 230 349

email: sales.se@norman.no Web: <http://www.norman.com/se>

### **Norman Data Defense Systems AG**

Münchensteinerstrasse 43, CH- 4052 Basel, **Switzerland**.

Tel: +41 61 317 2525 Fax: +41 61 317 25 26

email: norman@norman.ch Web: <http://www.norman.ch>

### **Norman Data Defense Systems (UK) Ltd**

Exchange House, 494 Midsummer Boulevard

Central Milton Keynes, MK9 2EA, **United Kingdom**

Tel. +44 08707 448044 / 01908 255990 Fax: 0870 1202901

email: norman@normanuk.com Web: <http://www.normanuk.com>

**Norman Data Defense Systems Inc.**

9302 Lee Highway, Suite 950A, Fairfax, VA 22031, USA

Tel: +1 703 267 6109, Fax: +1 703 934 6367

email: [norman@norman.com](mailto:norman@norman.com) Web: <http://www.norman.com>

**Training and Technical Support**

For training or technical support, please contact your local dealer or Norman ASA.

## System requirements

This version supports installation of Norman Security Suite v7 on Windows 2000, XP and Vista machines.

**Windows 2000**

CPU: any 450+ MHz Pentium-based platform

RAM: 256 MB

Other requirements:

Service pack 4

Update Rollup 1 for Windows 2000 SP4

Internet Explorer 6 or newer

100 MB of available disk space

**Windows XP**

CPU: any 450+ MHz Pentium-based platform

RAM: 256 MB (at least 512 MB recommended)

Other requirements:

Service pack 2

Internet Explorer 6 or newer

100 MB of available disk space

**Windows Vista**

CPU: 1 GHz 32-bit (x86) or 64-bit (x64) processor

RAM: 512 MB (at least 1GB recommended)

Other requirements:

Operating system and browser details

32 bit Windows Vista

Internet Explorer 7

100 MB of available disk space

## About this version

The current release is available in several languages. New languages are added at irregular intervals. Contact your Norman dealer for information about the Security Suite in your language. Check Norman's web sites for details, or contact your local dealer for more information about language versions.

## About this manual

This manual presents an overview of products, features and key functions in Norman Security Suite. Rather than presenting a complete walkthrough of all configuration options, this guide focuses on tips and procedures of a practical nature. Please refer to the online help for a detailed explanation of all available options.

## Technical support

Norman provides technical support and consultancy services for the Security Suite and security issues in general. Technical support also comprises quality assurance of your antivirus installation, including assistance in tailoring the Security Suite to match your exact needs.

Note that the number of services available will vary between the different countries.



# Contents

System requirements .....	iv
About this version .....	v
About this manual .....	v
Technical support .....	v
<b>About Norman Security Suite .....</b>	<b>9</b>
What is Norman Security Suite? .....	9
Virus & Spyware Protection .....	9
Personal Firewall .....	10
Parental Control .....	10
<b>Installing Norman Security Suite .....</b>	<b>11</b>
Wizards .....	14
<b>Virus &amp; Spyware Protection .....</b>	<b>15</b>
Installing and updating products .....	15
Update method .....	16
Select update method .....	16
Tray icons .....	17
Scanning .....	19
The On-access scanner .....	20
How to disable the On-access scanner .....	20
The On-demand scanner .....	21
Scan now .....	22
Setting up a scheduled scan .....	22
Enable the Screen saver scanner .....	24
Right-click scanning .....	26
The Command line scanner .....	26
Starting the Command line scanner .....	26

Exclude list .....	27
Create an exclude list .....	27
Scanning statistics .....	28
Internet protection .....	28
Advanced settings .....	31
Ports .....	33
Quarantine .....	34
Configure Quarantine .....	34
<b>Personal Firewall .....</b>	<b>36</b>
Switching mode between inexperienced and experienced user .....	36
Disable/Enable Personal Firewall .....	38
About rules .....	38
Create a rule - inexperienced mode .....	39
Create a rule - experienced mode .....	41
View traffic on your computer .....	41
Real-time log .....	41
Ports viewer .....	42
Useful facts about the Personal Firewall.....	44
<b>Parental Control .....</b>	<b>45</b>
Running the wizard .....	45
Users, Groups and Categories .....	47
Allowlist and Blocklist .....	48
How to create a user .....	48
Configure groups .....	49
How to configure group Child .....	49
How to configure group Teenager .....	50
How to schedule Internet access .....	51
<b>Support Center .....</b>	<b>53</b>
Help and troubleshooting .....	53
Contact information .....	54
Automatic repair .....	54
Using eLogger to monitor your installation .....	54
Uninstalling the Security Suite .....	55



---

<b>Appendix A .....</b>	<b>56</b>
What is a sandbox? .....	56



---

# About Norman Security Suite

## What is Norman Security Suite?

Norman Security Suite (NSS) is a software security package made up from three different security applications:

- Virus & Spyware Protection
- Personal Firewall
- Parental Control

Norman Security Suite is ready for use once you've installed it. The default configuration settings provide the protection you need, and you don't have to run through the configuration options to make the program operational. However, it's useful to have a perception of how things work and familiarize yourself with the basic functions.

This manual aims at pointing out certain useful features and provide some hints on how to get the most out of the program.

Note that you must run a wizard before you can start using the Personal Firewall and the Parental Control. Please refer to page 39 and page 45 respectively for more information.

## Virus & Spyware Protection

This antivirus program monitors your PC for malicious software, also referred to as malware. Malware is viruses, worms, trojans and other varieties of unwanted code. Spyware is not destructive like traditional viruses, but the consequences of revealing personal information inadvertently could be just as damaging. Norman's unique Sandbox provides proactive protection that identifies even unknown viruses.

⇒ For more information on Norman's Sandbox, refer to page 56.

Viruses can be automatically removed from hard disks, removable media, email attachments, etc.

The Virus & Spyware Protection application checks files when they are accessed, and possible viruses are removed automatically.

Since we encourage users to perform manual scans of the machine, you can choose Norman's screen saver which also starts a virus scan when

it's activated. When you resume work and a scan is aborted, it continues where it left the next time the screen saver kicks in. For regular manual scans, you can use the task editor and scheduler to define what area of the machine to scan and when.

This product is shipped with pre-selected settings that we consider sufficient to protect you against virus attacks. The modules can be configured so that you can set up the application to suit your exact needs.

## **Personal Firewall**

Whenever you're connected to the Internet, reading email or surfing the web, you make connections to other computers all over the world—and they connect to yours. This is where the trouble starts. By breaking into your computer, hackers may access your private documents, use your computer for their own acts of evil, or even render your computer useless by deleting important system files. The Personal Firewall controls in- and outgoing traffic on your computer based on a security policy which is established when you install the product (automatically or self-defined).

The Personal Firewall is first and foremost hacker protection.

## **Parental Control**

The Internet is not necessarily a good place to be, and there are some web sites we certainly don't want the youngest of the family to visit. Unless children and teenagers are under constant surveillance, they are likely to visit web sites with undesired content—deliberately or not. With Parental Control you can block access to certain categories of web sites, or even block all sites not explicitly approved. In addition you can restrict the time a user is allowed to surf on the net and specify what time of the day surfing is permitted. In short, you can customize a profile for the individual user based on age or other criteria you wish to take into account.

# Installing Norman Security Suite

1. Download the installer file from Norman's web site. The file is called NormanSecuritySuite\_SU\_RxXXX.exe, where 'x' represents the release number and 'XXX' the language version. In other words, NormanSecuritySuite\_SU\_R1ENG.exe is the English version of the first release of Norman Security Suite.
2. Double-click the file to start the installation and follow the instructions on the screen. We recommend that you read the Readme file in step 2.
3. In step 4 you are asked for a license key. If you previously purchased a product license, the license key holds information on the products you paid for.

**Tip:** If you have a copy of your license key in an email or some other electronic format, the easiest way is to copy the key into the license key field. Highlight the key and press Ctrl+C, place the cursor in the license key field and click Ctrl+V to paste in the key. Make

sure that there are no blank spaces included.



**Note:** If you don't have a key, you can leave this field blank and still install the entire suite. However, the License Wizard will regularly prompt you for a key and the product(s) will not be updated.

4. When you have entered a valid license key and pressed **Next**, this dialog appears:



**Note:** If you didn't enter a license key in the previous step, the default option is called **Complete** rather than **Typical**.

5. If you select **Typical** installation, all products covered by your license will be installed to c:\Program Files\Norman. You should select a **Custom** install if you don't want to install all products, or if you want to install to a different location than c:\Program Files\Norman.
6. The next dialog allows you to enable Norman's Screen Saver Scanner. This is a feature that scans your hard drive(s) when your system is idle and a 'normal' screen saver would be activated. This option provides a screen saver *and* a scanner. You can select/deselect this feature at any time. Please refer to 'Enable the Screen saver scanner' on page 24.



7. Click **Next** to complete the installation of the Security Suite.
8. When installation is complete, you will be asked to restart your computer. Don't restart until you're instructed to.

## Wizards

Norman Security Suite has three different wizards. The License Wizard (mentioned in step 3 above) that keeps track of the products you have a valid license for. The others are relevant if you have installed the Personal Firewall and/or Parental Control.

Once Norman Security Suite is installed, a wizard for setting up the Personal Firewall is launched (see page 36).

Finally, you must complete a wizard before you can start using Parental Control. Please refer to 'Running the wizard' on page 45.

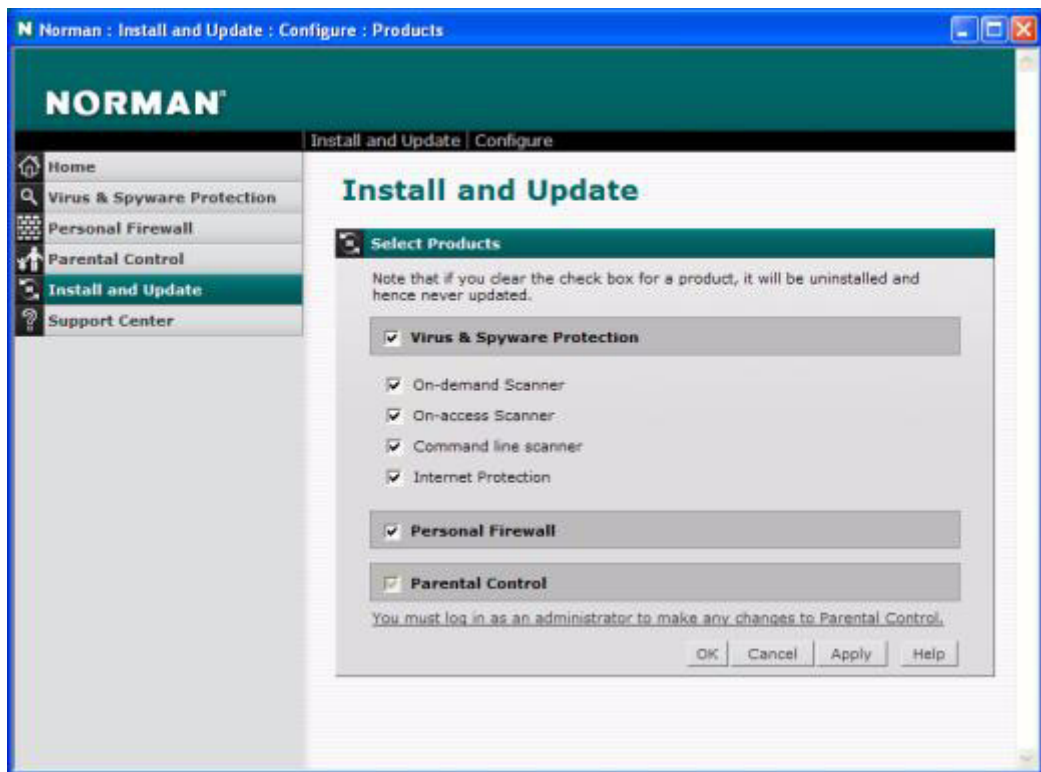
Common for all wizards are that they are easy to use and will handle basic product configuration.



# Virus & Spyware Protection

## Installing and updating products

Go to Install and Update | Configure | Products for a list of all available products.



If and when new products/components are added to the Security Suite they are downloaded automatically. You must however install new products manually by selecting them from this dialog. All selected products are automatically updated through the Security Suite's Internet Update.

Products not covered by your license will not appear in the list.

**Note well:** If you remove the check mark for a product, it will be **uninstalled** and therefore never updated.

## Update method

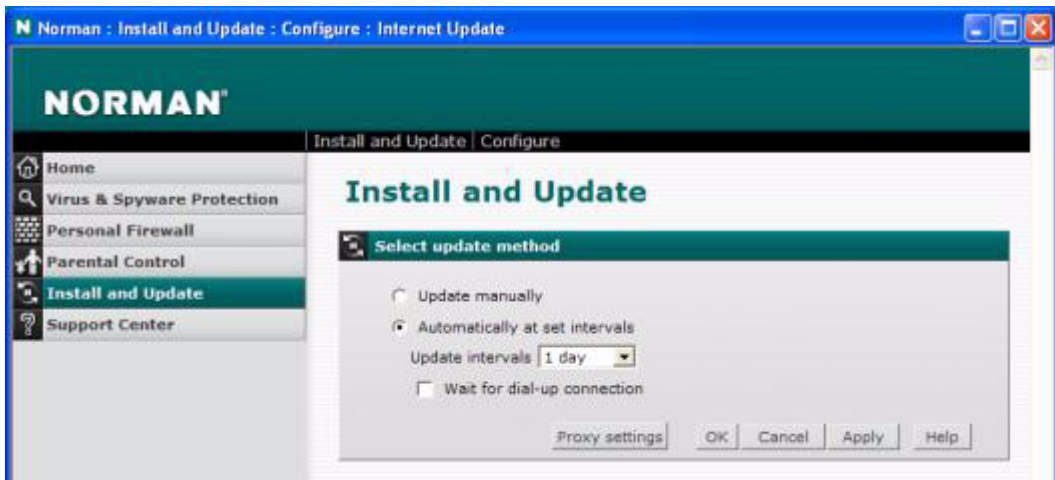
New malware appears every day, and Norman provides frequent updates to the virus definition files, as well as regular program updates of the Security Suite. You don't have to worry about the nature of the updates, as the Security Suite's agent handles everything and informs you if a restart of your computer is necessary, for example.

You can update the Security Suite via the Internet or the internal network.

In the **Install and update section**, you can update the entire Security Suite by one click on the **Update now** button.

## Select update method

1. Go to Install and update | Configure and click **Update method**. The following dialog appears:



2. The recommended update method is **Automatically at set intervals**. You can select this option if you have a permanent connection to the Internet. Click on **Update intervals** to set the frequency. The alternatives are *6 hours*, *12 hours* and *1 day*.

3. Select **Update manually** if you prefer to start the update mechanism manually from the tray or Start menu to check for updated packages, or use Windows' **Scheduled Tasks** utility (located in **Control Panel**).  
If you select this option, your installation is not updated automatically. You must run Internet Update manually, either from the tray menu or by selecting Install and Update | Update now.  
**Note:** If Internet Update has not been run for 24 hours, the program automatically checks for updates at start-up.  
**Tip:** If your machine is protected by a firewall or proxy server, you may have to click the **Proxy settings** button and enter the required information.
4. If you use a modem to connect to the Internet, select the **Wait for dial-up connection** option for daily checks for updates on Norman's servers. You just access the Internet like you normally do, and the program will figure out if updated files are available.  
If you connect to the Internet several times per day, the update mechanism checks for updates the first time you connect only. If you connect to the Internet once a week, for example, a check is performed once as soon as you're connected.
5. Click **Apply** when you're done.

## Tray icons



During setup, a Norman icon is placed in the system tray in the lower right-hand corner of the screen. This icon confirms that NSS is installed on this machine.

When you right-click this icon, the following menu appears:



Note that the options in this menu will look different depending on which NSS products are installed.

The items in the list with an icon in front of them are copies of the items that at any time appear on the Start | Programs | Norman Security Suite menu.

This is a shortcut to Norman Security Suite's main modules, as

well as some typical tasks. You can **Start/stop the on-access scanner** or **Disable/enable the Personal Firewall** by a simple mouse click. Select **Contact us** to display contact information for our offices and distributors on Norman's web site, or view the license. Finally, you can view update status for the Norman product(s), including key information for the virus definition files.

This function is also the originator of messages regarding outdated virus definition files, expiration of licence period, and other information.

### Warnings

The Norman icon also provides information regarding the state of your Security Suite installation. This icon denotes that some of the components currently running are outdated. If the Norman 'N' appears with the red symbol blinking, place the pointing device on the symbol to find out which component that needs updating or if there are other error situations.



**Note:** During startup, the red symbol is visible until all modules have started. The older and slower the machine, the longer it takes for all modules to load. However, the "normal" symbol should appear after a maximum of 1-2 minutes.

**For Windows XP and Vista users:** Microsoft included its "Security Center" with options and features for Firewall, automatic updates and virus protection. Norman is one of the AV vendors that the operating system detects. If the virus definition files are outdated or the On-access scanner is not running, you will also receive a warning from



Windows that something is wrong. The Security Center symbol appears, and you can click on it to view and edit the Windows settings.

If the warning triangle icon appears in the system tray, it signifies that one of these situations have occurred:

1. The On-access scanner is installed, but has been manually disabled. To start the On-access scanner, select the shortcut from the right-click menu, or go to the Virus & Spyware Protection main console. See ‘The On-access scanner’ on page 20 for details.
2. You have probably selected **Reboot later** on a previous prompt, and the Security Suite is waiting for a reboot.
3. An installation error that a reboot might fix.

### Outdated virus definition files



A *blinking* yellow triangle signifies that the virus definition files are outdated, i.e. they are at least ten days old. The same happens if the On-access scanner is stopped/paused from the tray menu.

### Informational icons



When the Norman icon appears with a cog, Norman Program Manager is working with the program, most likely an update. We do not recommend that you turn off your machine when NPM is working, i.e. while this symbol is visible.

**Note:** An update shouldn't take more than 5-10 minutes. If the cog icon is present for a longer period of time, something might be wrong with the installation. In that case, try the **Repair** option available from *delnvc5* and described on page 54.

**Tip:** You can always place the cursor on any type of icon in the system tray for an explanation of errors or messages.

## Scanning

The Security Suite features two main scanners—the On-access scanner and the On-demand scanner—as well as different scanning methods. Both scanners employ the unrivaled Sandbox, a feature that detects new and unknown viruses. Select this option if you want the Virus & Spyware Protection application to look out for unknown virus variants. By default, the Sandbox option is on for both scanners. Scanning time

increases somewhat when the Sandbox is active, but it is not likely to affect the overall system performance significantly.

If a scanner detects a virus or other type of malware, it will try to clean the infected file or—if the file has no other than destructive purposes—delete it entirely.

## The On-access scanner

The On-access scanner is working in the background and offers automatic protection of your system. It is an essential virus control component and should therefore be enabled at all times. If the On-access scanner is stopped/paused from the tray menu, a blinking, yellow triangle appears in the system tray. See 'Warnings' on page 18.

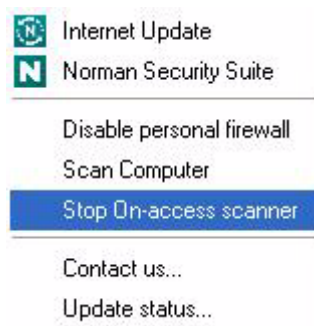
Whenever a file is accessed in a read/write operation or a program is executed, the On-access scanner is notified and scans the file on the fly, if configured to.

Like the On-demand scanner, the On-access scanner detects and repairs all types of viruses. Whenever possible, an infected file is repaired before the file is handed over to the application. Access to the infected file is denied if repair fails.

## How to disable the On-access scanner

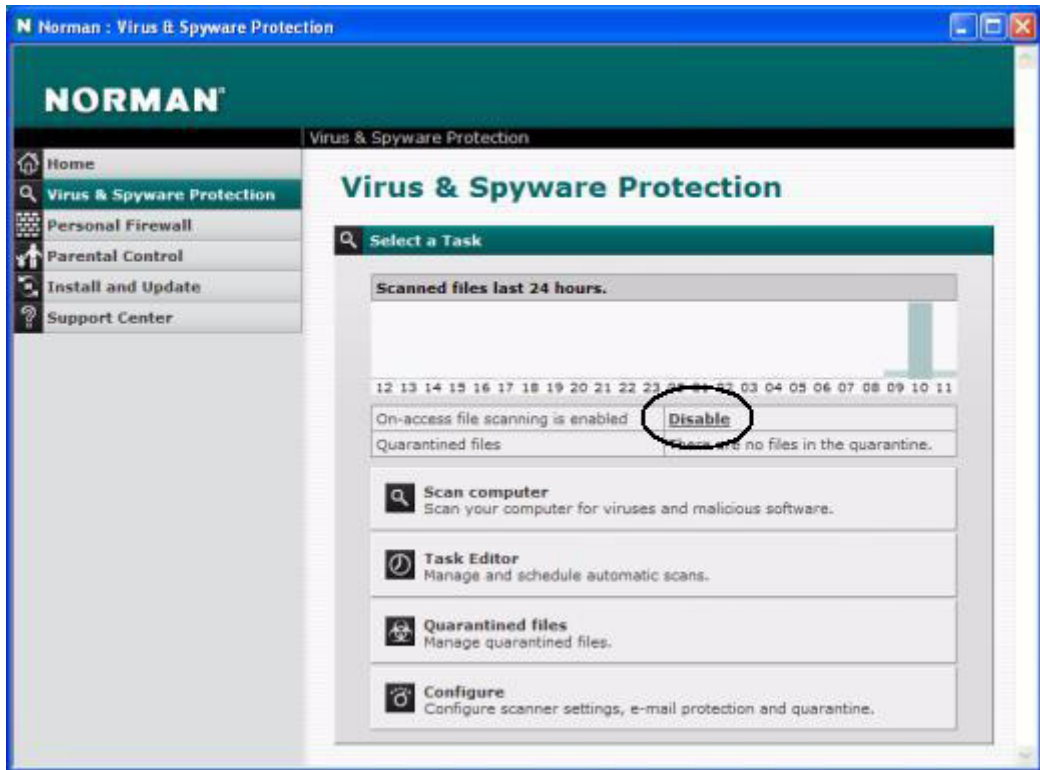
We recommend that the On-access scanner is enabled at all times. However, if you for some reason need to disable it, this is what you do:

1. From the tray menu, select **Stop the On-access scanner**.



If you don't manually start the scanner again, it will be enabled the next time you restart your computer or when an update is installed.

2. From the Virus & Spyware Protection main page, click **Disable** for **On-access file scanning is enabled**.



3. Note well that the configuration has now changed. Disabling the On-access scanner from here is the same as removing the check mark for **Enable On-access scanner** under Virus & Spyware Protection | Configure | Scanners | On-access scanner. The scanner remains disabled until you manually enable it again.
4. If you disable the On-access scanner in this way, no warning is issued by the Security Suite. However, Windows' Security Center will warn.

## The On-demand scanner

Use the On-demand scanner for periodic scans of entire drives, selected folders or files. Scanning an entire hard drive is a time-consuming exercise, so we encourage you to set up scheduled scans using the Task

Editor, and enable the Screen Saver Scanner. Thus on-demand scans are performed automatically during periods of low activity. Finally, the On-demand scanner can be launched by right-clicking a file system object.

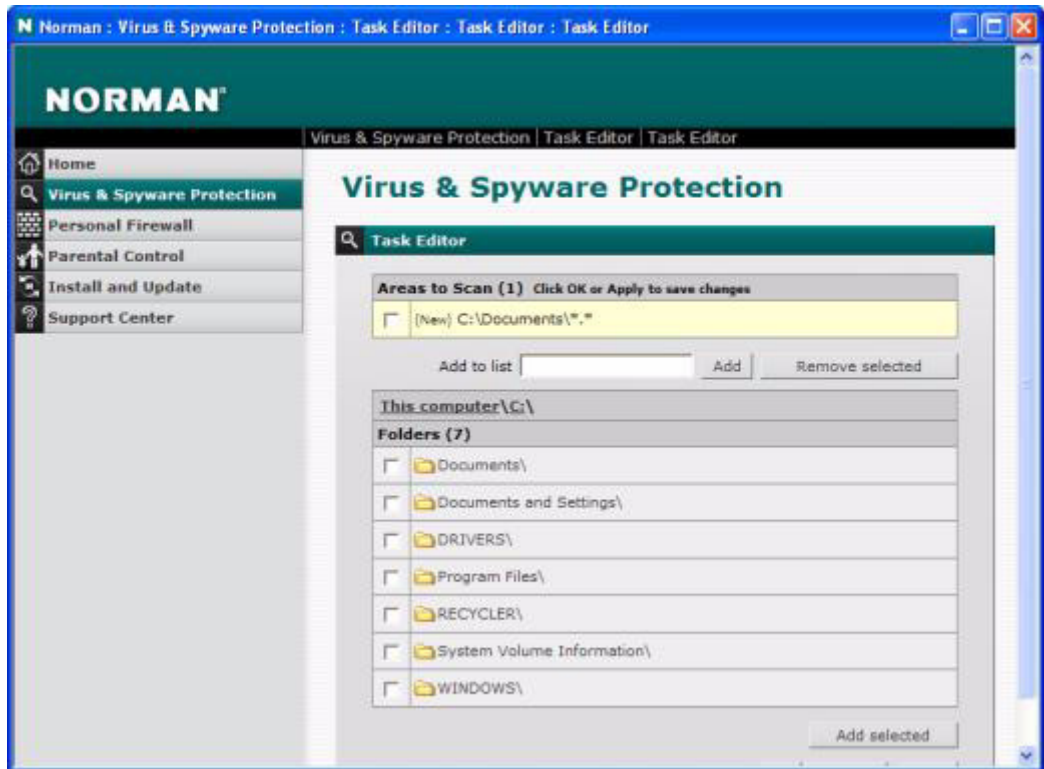
## Scan now

From the Virus & Spyware Protection main console, click **Scan computer**. The On-demand scanner launches a scan of all hard drives on the system.

## Setting up a scheduled scan

1. Select **Task Editor** from the Virus & Spyware Protection main page.
2. Then click **Create a Task**.
3. Enter a task name, for example *Documents*.
4. Specify area to scan. Select **Scan selected files and folders** and click on the corresponding link:





5. Select the drive and folder(s) to scan and click **Add selected**. The area you just selected appears in a list at the top.
6. Click **OK**.
7. You're returned to the previous dialog. Click **Next**.
8. Select frequency for the task (Once, Daily, Weekly, Monthly) and start date and time:



9. Click **Next**.
10. The last dialog displays a summary of the newly created task. Click **Back** to change your settings, **Cancel** to abort or **Finish** to save the task.
11. All scheduled tasks are displayed in a list in the Virus & Spyware Protection | Task Editor dialog.

### Enable the Screen saver scanner

When you select the Screen Saver scanner, a virus scan of your system is performed during idle periods. The On-demand scanner will start a scan of all hard drives once the screen saver is launched. If the scan is aborted before it's finished, it will start scanning from where it was stopped the next time it's activated.

1. Go to Virus & Spyware Protection | Configure and click **Enable screen saver scanner**. The following dialog (in Windows' Control Panel) appears:



2. Select **Norman Screensaver** as “Screen saver”. When you’ve made possible desired changes to the settings, click **OK**.
3. In the next system idle period, the On-demand scanner will start scanning your hard drives—displaying the progress continuously.

Note that a screen saver scan employs the settings specified under Virus & Spyware Protection | Configure | Scanners | On-demand scanner.

## Right-click scanning

You can also launch the On-demand scanner by right-clicking a file system object in Windows Explorer or on the desktop, for example, and then selecting *Scan for viruses* from the menu.



## The Command line scanner

The Command line scanner is an alternative to the GUI-based scanner and offers the possibility of running batch jobs and other scanning tasks from the command line. The Command line scanner is a good alternative for those familiar with this environment.

The command line scanner has the same basic functionality as the menu-driven scanners and is not dependent on any other modules. It can also be run from batch files.

### Starting the Command line scanner

1. From the DOS prompt, go to the directory where the Virus & Spyware Protection application resides (the default location is `...\norman\nvc\bin`):
2. The syntax is:

```
nvcc [drive]:[path] [/parameters] [Enter]
```

A space must precede each parameter that you use.

Simply select the combination of parameters that you wish to use and specify them on the command line.

3. For a list of available parameters, enter `nvcc /?`

## Exclude list

You may want to speed up the scanning process by excluding certain files from scanning. Note that excluding files or areas from scanning is a decision at the expense of security.

Files on the Exclude list are not scanned. Reasons for not scanning certain files may be that they trigger false alarms, or they are too time-consuming to scan. At any rate, we recommend that you scan files on the exclude list regularly by running scheduled or on-demand scans (page 21).

You can create exclude lists for the On-access and the On-demand scanners.

### Create an exclude list

1. Go to Virus & Spyware Protection | Configure | Scanners.
2. Select the relevant tab (On-access scanner or On-demand scanner).
3. Adding separate files: in the *Add to list* box, type in the path and file name and click **Add**, and then **Apply**.
4. Adding disk drives or folders: select drive letter and click **Add selected**, or click the drive letter and browse for the folder(s) you wish to exclude from scanning. Click **Add selected** and then **Apply**.
5. The newly added drives, folders or files appear in the list in the upper part of the dialog.
6. To remove entries from the list, select the relevant entry and click **Remove selected**. Click **Apply** when you're done.

**Note:** NSS does **not** check if the files, folders or drives you add to the exclude list really exist. Be careful to enter the correct names and paths.

## Scanning statistics

At the top of the Virus & Spyware Protection “home” page there is a graphical representation of scanned files and detected infections over the past 24 hours. The current hour is at the far right, i.e. the example below covers the period since 3 PM yesterday till 2 PM today. The statistical numbers represent the activity of the On-demand and the On-access scanner.

Place the cursor on a column to view details for that particular hour. In the example below 21,663 clean files were scanned between 11 AM and noon. One or more infections were detected between 2 PM and 3 PM, denoted by the red color for that period. Place the cursor over that period to check how many infected files were found, and if they were cleaned.



## Internet protection

Norman Internet Protection (NIP) is a filter that protects against viruses that spread through

- Internet mail,
- news readers,

The majority of viruses reported today use mechanisms that enable them to spread through e-mail. NIP is a module designed to intercept

incoming and outgoing mail and news—stripping or blocking all infected attachments for undesired content.

NIP is both capable of scanning e-mails for known viruses and block file attachments, depending on content and file extensions.

All scanning options in the Internet Protection module are preselected:



The option **Use Sandbox** activates Norman's sandbox functionality to detect new, unknown viruses. The sandbox is particularly tuned to find new email-, network- and peer-to-peer worms and file viruses, and will also react to unknown security threats.

Scanning time will increase when this option is selected, but it is not likely to have a significant effect on performance. For more information about the sandbox, please refer to 'Appendix A' on page 56.

**Incoming / Outgoing e-mail** scan all e-mail that you receive and send to others. Even your best friend, closest business associate or yourself may be ignorant of a virus infection.

The option **Newsgroups** scans the traffic generated between your computer and the other participants in the group/forum you are active in.

**Instant messaging (received files)** scans file transfer traffic during instant messaging sessions with MSN Messenger and Windows Messenger. When this option is selected, NIP will scan incoming files for malware. If a file is infected, a pop-up message will warn about the incident.

Only file transfers are scanned, so infected links still pose a threat.

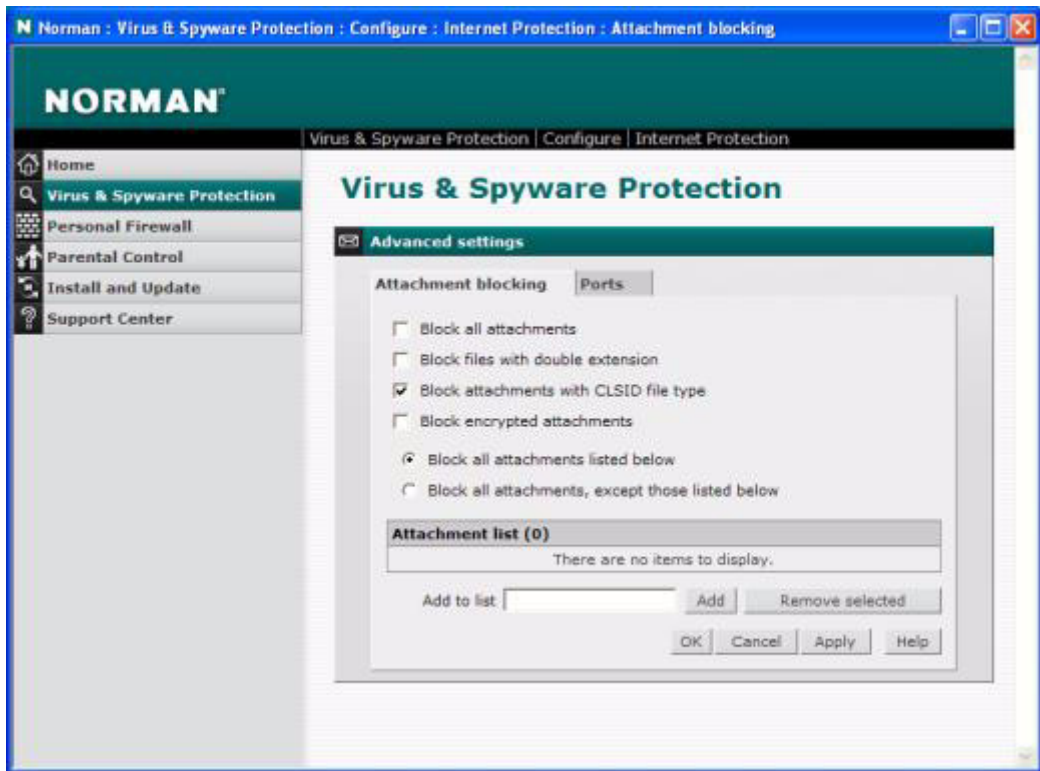
Note that the files that are transferred will be scanned when they are written to the directory `...\Temporary Internet Files`. If malware is detected, it is probably a `.tmp` file that is quarantined. To restore a quarantined `.tmp` file, select the desired file, choose the **Save as** option from the right-click menu and save the file with its original name and extension.

⇒ See 'Quarantine' on page 34.



## Advanced settings

Click the **Advanced settings** button to view this dialog:



This is a short explanation of the available configuration options:

**Block all attachments:** all attachments are blocked.

**Block any attachment with double extensions:** many worms and e-mail viruses apply a technique where an additional extension is added, for example <filename>.jpg.vbs. Most e-mail clients will hide the last extension so that the attachment appears to only have the extension .jpg. However, this feature is not only used by viruses—legitimate files with names like myfile.hlp.zip and todolist 20.dec.doc are both treated as double extensions.

**Block any CLSID extensions** (default option): some worms and e-mail viruses apply a CLSID technique to fool e-mail scanners and blocking software. They take advantage of a feature in Windows which

makes it possible to replace an .exe extension with a {...} extension and thus evade blocking of .exe files. Since there is no reason for legitimate attachments to use this type of extension, this behavior is blocked by default.

**Block encrypted attachments:** depending on the tools used, compressed and encrypted files are generally harder to scan for viruses than plain file attachments. Therefore NIP offers the option of blocking such attachments altogether.

**Block all attachments listed below** (default option): all names that you **Add** to the list are *blocked*. Enter a specific name, or use wildcard ('\*') to identify attachments to stop. See "Attachment list" below.

**Block all attachments, except those listed below:** all names that you **Add** to the list are *accepted*. Enter a specific name, or use wildcard ('\*') to identify attachments to accept. See "Attachment list" below.

**Note:** It is *very* important that you distinguish carefully between these two options, as they represent two extremes: *block* all entries in the list, or *accept* all entries in the list.

#### Attachment list

Use this function to explicitly select attachments you want to block — or certify. You can enter the exact name of an attachment, or use wildcard ('\*') to block certain extensions. To block all .exe files, for example, click on **Add** and enter \*.exe. Click **OK**, and the entry appears in the list box, where you later can edit or remove it.

## Ports

Among the numerous protocols for communication between computers, there are some that are vital for Internet use. For standardization reasons, protocols have pre-assigned port numbers.



### Port numbers

In the section 'Internet protection' on page 28, you selected which Internet traffic you wish to scan. This dialog identifies the protocols needed for sending and receiving e-mails, for example, and the corresponding port number on the PC, according to industry standards.

If you have assigned different port numbers to one or more of the supported protocols listed here, you must enter the **actual** port number for the affected protocol(s).

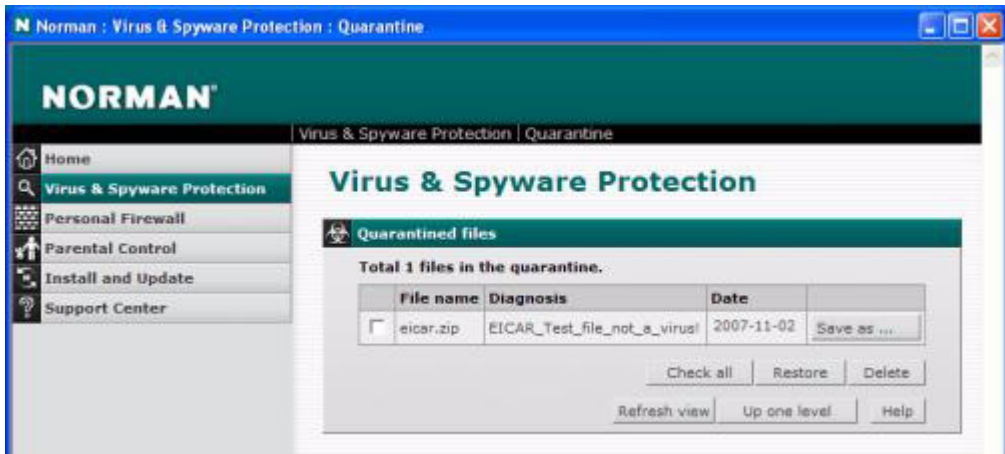
The options presents the type of traffic they will scan and the protocol name for these functions. The functions/protocols below are those supported presently. The list is likely to be updated whenever necessary:

- Incoming e-mail (POP3)
- Outgoing e-mail (SMTP)
- Newsgroups (NNTP)

## Quarantine

The Virus & Spyware Protection application will try to clean infected files before they are deleted and/or quarantined (depending on your configuration). Quarantined files are either infected or have been blocked by the Internet Protection feature. When you select Virus & Spyware Protection | Quarantine, you can view all quarantined files:

**Note:** A copy of a deleted or blocked file is quarantined by default.



Infected files that have been quarantined appear in this list, provided that you have configured the program to do so.

When the On-access scanner detects that `c:\eicar.com` is infected, it is moved to quarantine. However, if the On-access scanner detects `c:\copy of eicar.com` and this file is identical to `eicar.com`, `copy of eicar.com` is not quarantined, but deleted. If `copy of eicar.com` resides on `c:\another folder\` it is, however, moved to quarantine because of the new location. This method is implemented to avoid that the quarantine is crammed in a situation where a virus has written several copies of the same file to the same area of the disk drive.

### Configure Quarantine

1. Select Virus & Spyware Protection | Configure | Quarantine.

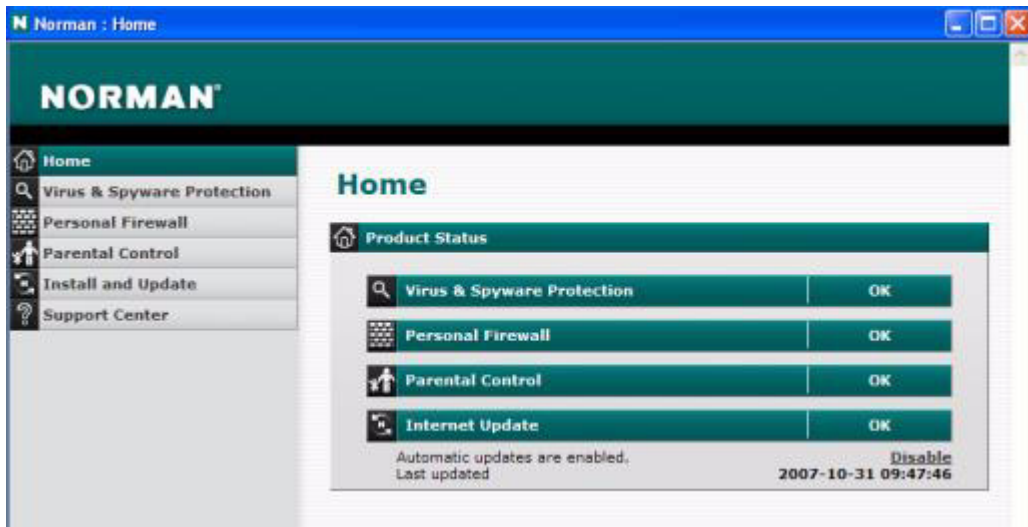
2. Select if you want to **Back up all files to quarantine before repair** and **Move unrepairable files to quarantine**. Both options are preselected and recommended.
3. Then specify minimum and maximum time files should be held in quarantine, and how much disk space they are allowed to occupy. A file which hasn't reached the minimum time will not be deleted though—then the reserved disk space allocated for quarantined files will be expanded.
4. Click **Apply** when you're done.

# Personal Firewall

When you install the Personal Firewall, you must run the installation wizard which establishes basic rules for NPF automatically, such as granting Internet access for the relevant applications. You can always change automatically generated rules later, using the Rule Editor.

It is highly recommended that you run the installation wizard, which offers different steps for experienced and less experienced users. The purpose of the wizard is to identify programs with a legitimate need to access the Internet and to create rules for these applications.

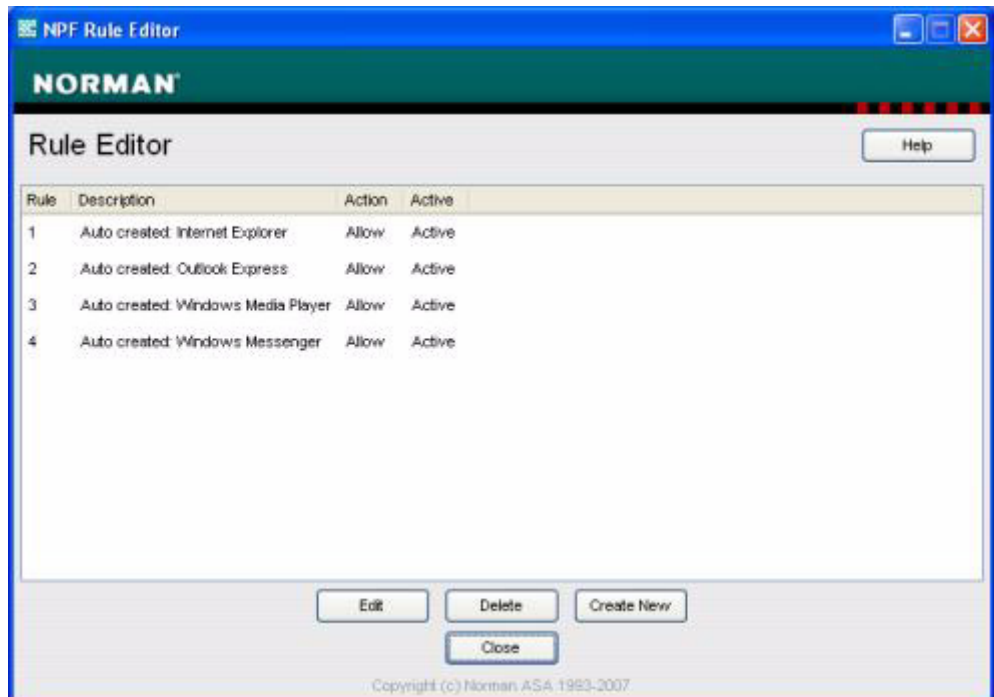
When you have completed the installation wizard, select **Personal Firewall** from the Security Suite's home page:



## Switching mode between inexperienced and experienced user

Depending on which version of the Personal Firewall's wizard you selected, you are defined either as inexperienced or experienced user. The option **Use advanced rule editor** (Personal Firewall | Configure | Advanced settings) is automatically selected if you ran the

“experienced” wizard. Clear the check mark for this option to change level to inexperienced user. The difference between the two categories is the degree of assistance you get when you create new rules or change existing rules. As inexperienced user a rule wizard will guide you through the rule handling. The experienced user is presented to this Rule Editor screen when clicking Personal Firewall | Configure | Rule Editor:



## Disable/Enable Personal Firewall

You can disable/enable the Personal Firewall by right-clicking the tray icon. Select **Disable Personal Firewall**. This entry changes to **Enable Personal Firewall** when the application is disabled.

**Note:** This option is not available on Windows Vista, where you must disable and enable the Personal Firewall from the console.

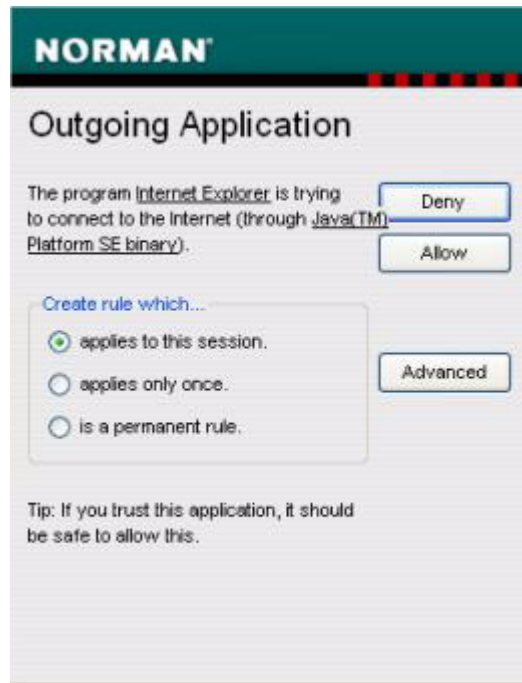


Windows' Security Center also issues a warning when the firewall is disabled.

## About rules

Rules are necessary to allow “trusted” applications Internet access, like so many programs rely on these days. The Personal Firewall detected “trusted” programs installed on your machine that need to be online, like web browsers and email clients, and established rules for them when you ran the wizard. However, you may have programs installed that the firewall didn't recognize or were acquired after you installed the firewall. When such a program tries to connect to the net, the firewall produces a pop-up that informs about the action and let you decide if you will allow or deny the action:

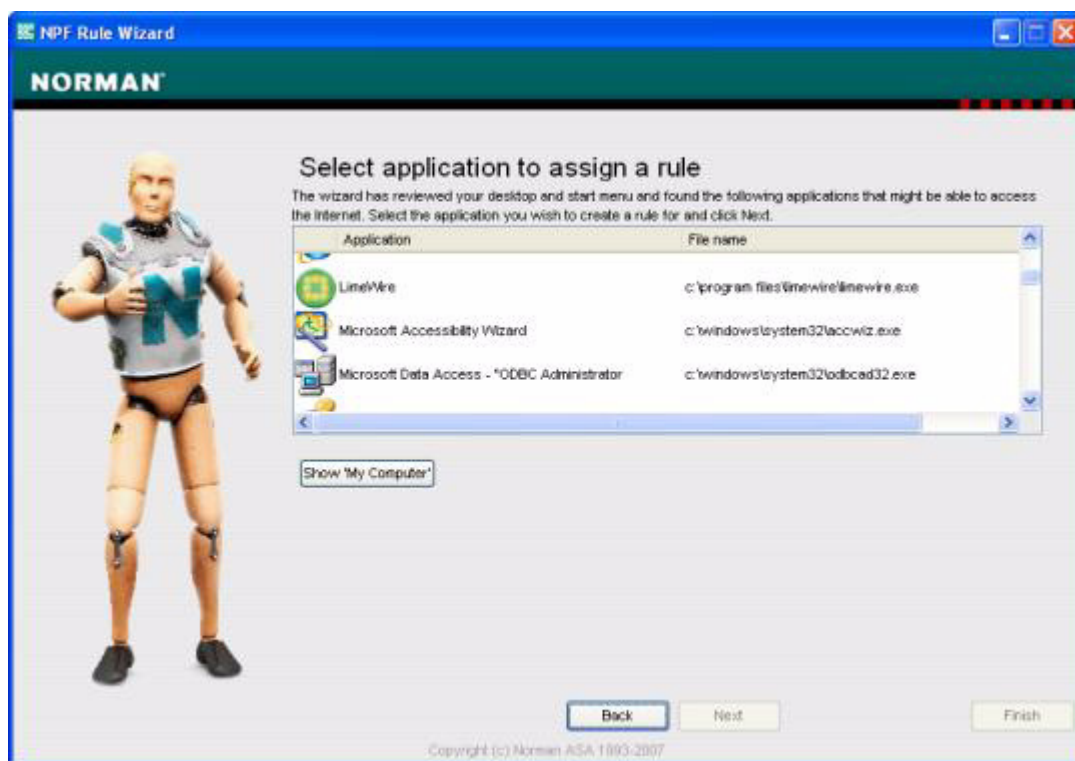




The Personal Firewall does not allow you to create *incoming* rules. Incoming rules are handled by the firewall's Server Mode awareness, which dynamically and automatically creates incoming rules based on Server Privileges. This is an intelligent mechanism in the firewall that evaluates attempts from the outside to listen on a set of ports. Legitimate requests are granted access only for the relevant ports, and they are automatically closed when they are no longer needed.

### Create a rule - inexperienced mode

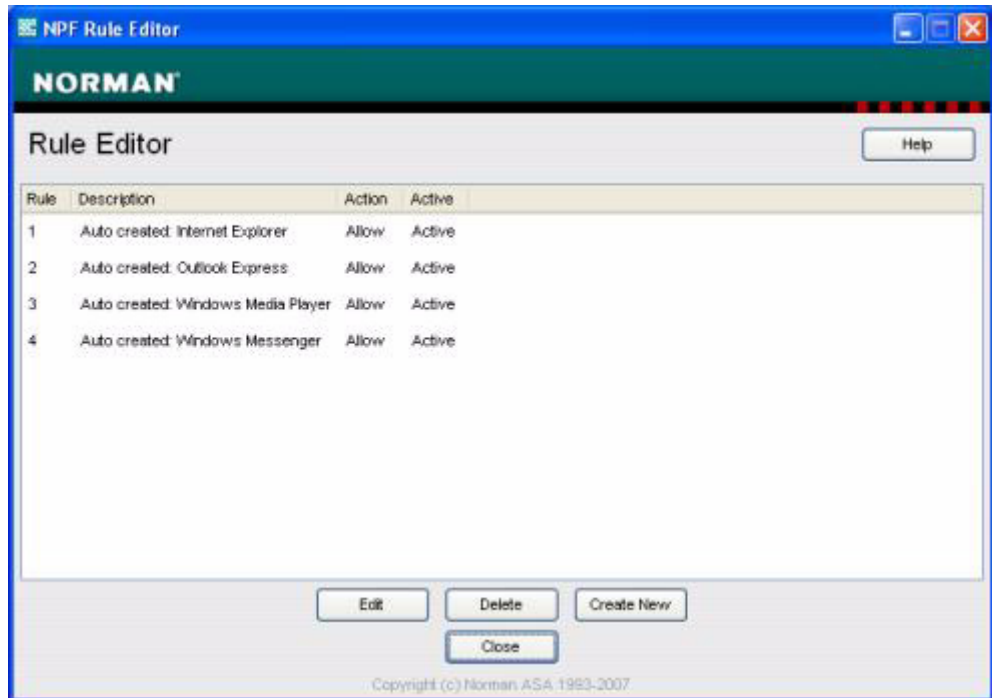
1. Select Personal Firewall | Configure | Rule Editor. The Rule Wizard appears.
2. Select **I want to create a new rule** and click **Next**.
3. A list of eligible applications is presented:



4. Select an application by clicking on it, or select **Show My Computer** if the program you're looking for is missing from the list. Click **Next**.
  5. Decide if this application should be **Allowed** or **Denied** access to the Internet. Click **Next**.
  6. Determine if this is a server application or not. Server applications make your computer behave as a server by holding ports open, allowing other computers to connect to yours. If in doubt, select **No**. Click **Next**.
- Tip:** If you change your mind, you can always go back and change a rule later.
7. A summary dialog appears. When you click **Finish**, the rule is generated and takes effect immediately.

## Create a rule - experienced mode

1. Select Personal Firewall | Configure | Rule Editor. A dialog listing existing rules and their status appears:



2. Click the **Create New** button.
3. Complete the required fields and click **OK**.

**Tip:** There's a detailed description of all fields in the online help.

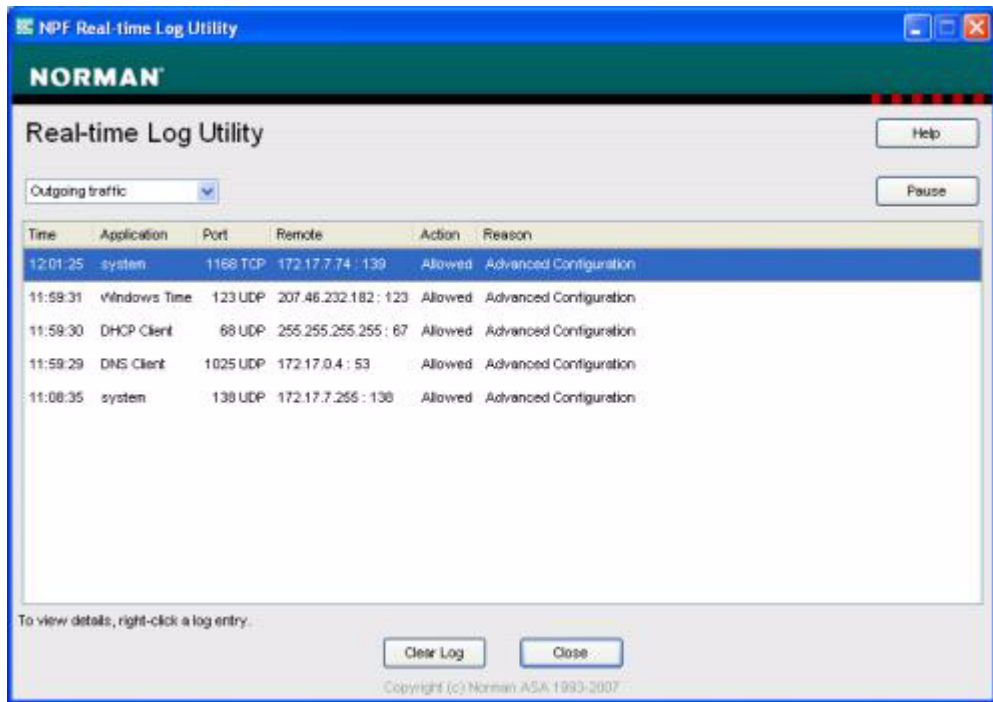
## View traffic on your computer

### Real-time log

The Personal Firewall employs advanced stealthing techniques that make your computer invisible and undetectable from the Internet. You can keep an eye on activities on your own machine using two other features: the *real-time log utility* and the *advanced ports viewer*.

1. From Personal Firewall | Expert Tools, select **Real-time log utility**. The following dialog appears with an overview of outgoing

applications and key information for these:

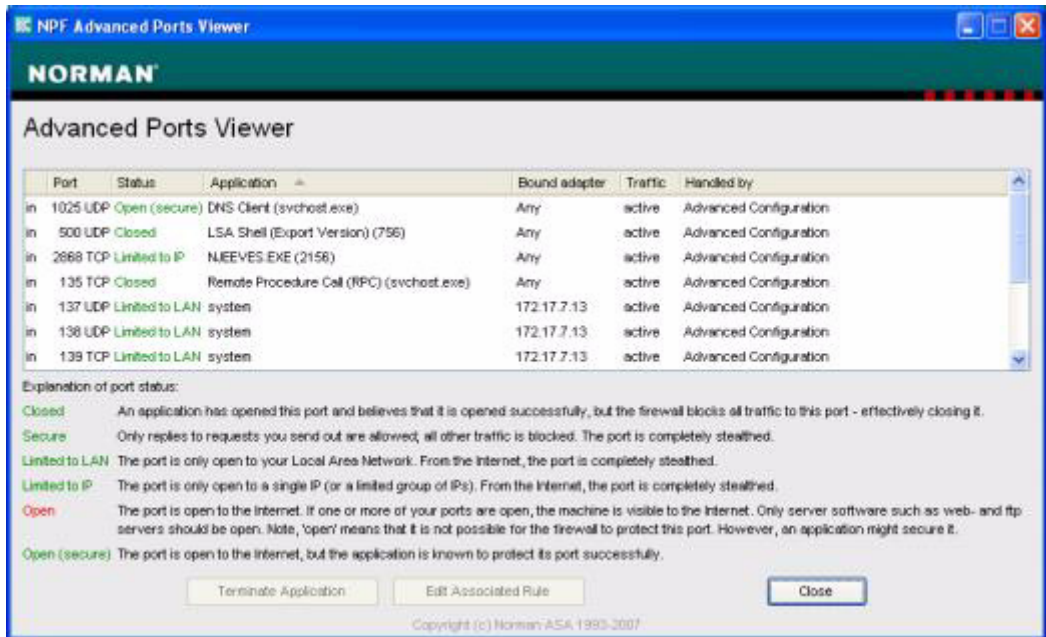


2. Right-click an entry to view details and possibly change the configuration for this application.
3. From the drop-down menu you can change between the following views: *Outgoing traffic*, *Incoming traffic*, *Server privileges requests* and *Status messages* from the firewall.

**Tip:** If you select *Incoming traffic*, you can see attempts to connect to your computer that were denied, and why.

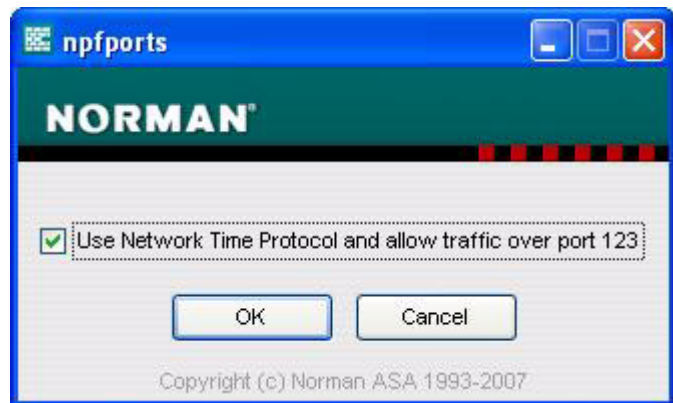
## Ports viewer

1. From Personal Firewall | Expert Tools, select **Advanced Ports Viewer**. The following dialog appears with an overview of which application is using which port on your machine, status, traffic, etc:



2. The bottom half of the screen contains explanations of the different status types.
3. You can highlight an entry and stop the application by clicking the **Terminate Application** button.

**Tip:** Highlight an entry and click the **Open Advanced Configuration** button:



To change an application's configuration from allow to deny, remove the check mark and click **OK**. Alternatively, insert a check mark to allow a denied application access to the Internet.

Note that **Terminate Application** and **Edit Associated Rule** only apply to entries "handled by rule".

The **Open Advanced Configuration** option is only available for rules handled by "advanced configuration".

## Useful facts about the Personal Firewall

You have seen that the Personal Firewall's rule wizard automatically can create rules for applications' behavior with regard to accessing the Internet. We have also established that there are different modes for experienced and inexperienced users, and that the firewall features a "server mode awareness". You can create and change rules and view details for traffic and port activity. In addition, Norman Personal Firewall offers:

- Launcher protection, that detects attempts from an application to launch itself through another application.
- Stealth launch protection, that uncovers malicious applications attempting to access the Internet via other applications. The Personal Firewall keeps track of all parent applications.
- Process hijacking protection, which prevents that malicious applications hijack a "trusted" process for dll or thread injection.
- Full stealth mode, that ensures that *all* ports on your computer are completely invisible from the outside.
- Advanced svchost handling, where each svchost service has separate rules rather than one general rule to cover the grouping of services that each Svchost.exe session can contain.
- Anti-pharming, implemented through protection of the HOSTS file and therefore eliminating the most common pharming attack method.

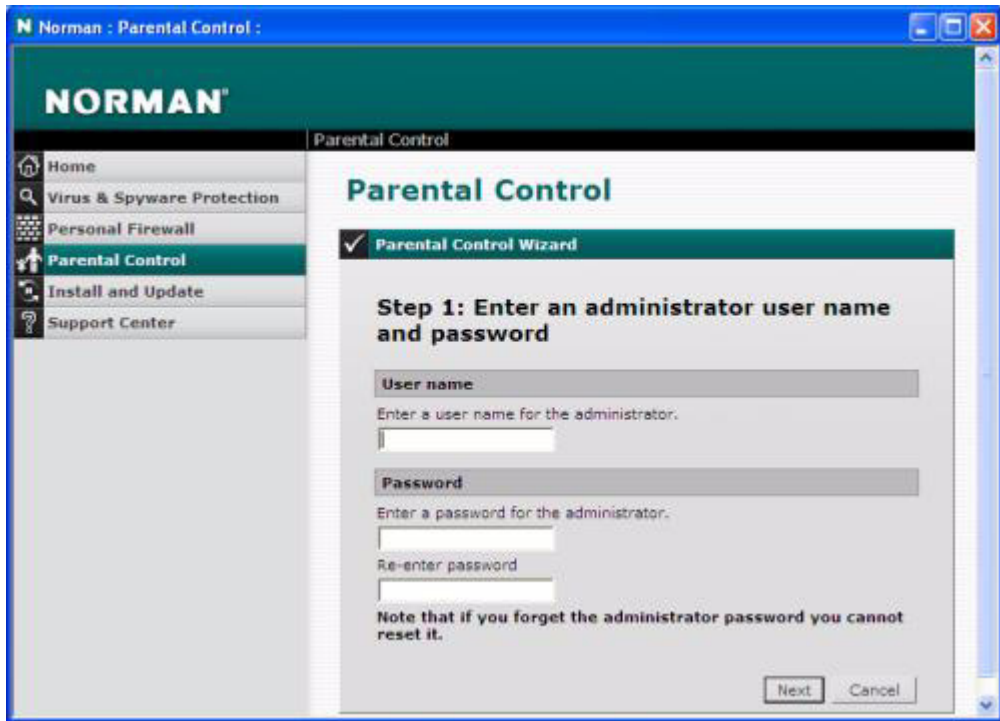
# Parental Control

The purpose of Parental Control is to shield the young ones from the shady sides of the Internet. It's no secret that there is an abundance of bizarre web sites inappropriate for kids (and most adults too, for that matter). The Internet is not censored, but you can introduce your own censorship to protect your children from viewing web sites with undesired content—deliberately or not. With Parental Control you can block access to certain categories of web sites, or even block all sites not explicitly approved. In addition you can restrict the time a user is allowed to surf on the net and specify what time of the day surfing is permitted. In short, you can customize a profile for the individual user based on age or other criteria you wish to take into account.

After you have installed Norman Security Suite, you must run a wizard before you can start using Parental Control. The reason is that only the administrator can configure the program, like setting the default profile, create users, etc.

## Running the wizard

1. When you have installed Norman Security Suite, status for Parental Control on the Home page is **Information**. Click on this link to launch the wizard.
2. The first dialog informs you about the scheme of the wizard and which steps are included. Click **Next**.
3. In this step you should enter a name and a password for the administrator. Only this user is allowed to configure Parental Control. Make sure that you pick a password you won't forget since it cannot be reset. *The password is case sensitive.* Click **Next**.



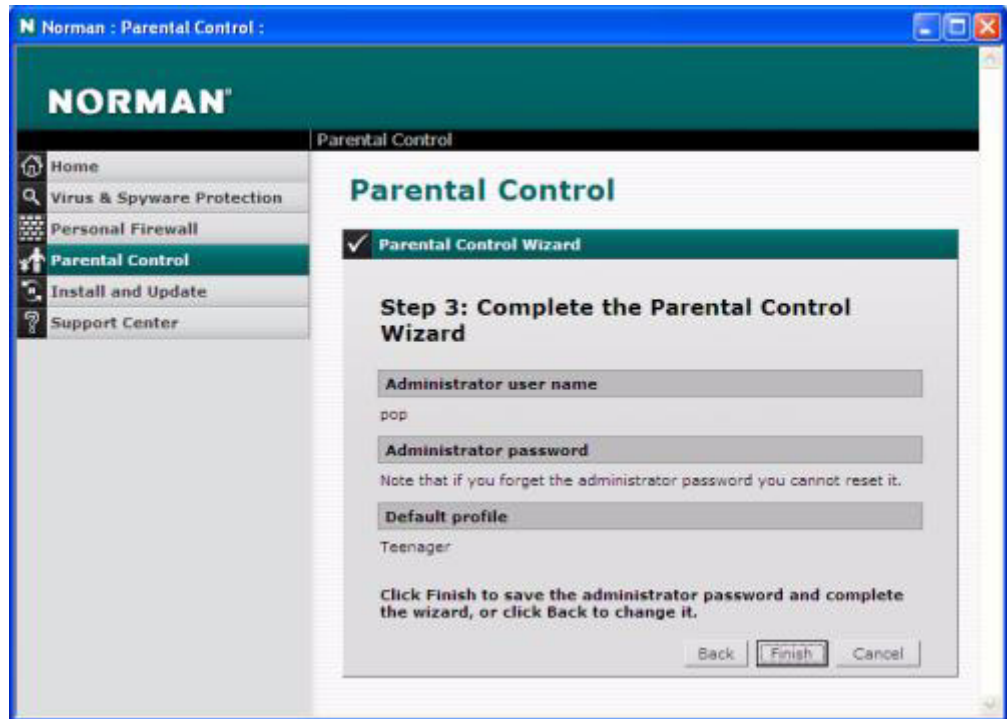
4. Now select default profile. Parental Control will fall back on this profile after the specified idle time. Idle time is a period where there is no activity on the system, i.e. no keyboard strokes and no mouse movements. When you've completed the wizard, you can log in as administrator and decide when Parental Control should fall back on default profile when the PC is idle.

You can select **Child** or **Teenager** as the profile Parental Control should fall back on after the specified idle period.

A user in the **Child** category is only allowed to view the web pages that the administrator types in the Allowlist. A user in the **Teenager** category is restricted by the category filters (see page 47).

5. In the final step you can view and confirm your choices. Click **Back** to make changes or **Finish** to complete the wizard with the current settings:





6. Click **OK** in the next dialog, and the administrator login appears. Log in with the password you entered in Step 1, and you are ready to configure the product as you like.

## Users, Groups and Categories

When you create a user, you must complete a couple of mandatory steps where you assign group and password for the new user.

There are three *groups*: Adult, Teenager and Child.

**Adult:** No restrictions - the user can access any web site.

**Teenager:** Restricted by the category filters (see below).

**Child:** Only allowed to view the web pages that the administrator types in the Allowlist.

*Categories* are based on a wide range of terms and expressions that enable the Parental Control to identify a web page as predominately sex oriented, for example. The program applies a technique that requires the presence of a set of conditions for a web page to be classified as

belonging to a category. The terms that the categories are based on are not accessible for viewing or editing.

There are four categories for the group Teenager that will block access to web pages with contents of the types *sex*, *gambling*, *weapons* and *drugs*.

All categories are by default on, but the administrator can uncheck the one(s) that should be allowed.

## Allowlist and Blocklist

For users in the Child group an allowlist must exist, since only the web addresses on this list are possible to view. For users in the Teenager group you can create both an allowlist and a blocklist, but for this group it is optional to use these lists.

In addition, you can allow one or more categories for the Teenager group. See 'How to configure group Teenager' on page 50.

**Note:** Both the allowlist and the blocklist affect **all** users within the group.

## How to create a user

1. Select Parental Control | User configuration | Add user.
2. In the next dialog, select which group the new user should be based on. The default group is Child. Click **Next**.
3. Enter user name and password for the new user. Click **Next**.



4. You'll receive a confirmation that a new user is created. Click **OK**.

## Configure groups

Since the group Adult has no restrictions, only Child and Teenager can be configured. If a user who is assigned to group Child should be able to access the Internet at all, you must specify which web pages this user is allowed to access.

### How to configure group Child

1. Select Parental Control | Group configuration | Child.
2. Click **Configure allowlist**. Because all web pages for the group Child are blocked unless they are explicitly permitted, there is no Blocklist or Category for this group. The following dialog appears:



3. Type in the web address you wish to allow in the *Add to list* box and click **Add**. Valid formats are:

http://www.newspaper.com  
www.newspaper.com  
newspaper.com

Wildcards (\*/? ) are not supported.

**Tip:** If you grant access to <http://www.newspaper.com/kidsstuff> it does not permit access to <http://www.newspaper.com>. If [newspaper.com](http://www.newspaper.com) is added, all sub domains of this web address are allowed, like [news.newspaper.com](http://news.newspaper.com), [cartoon.newspaper.com](http://cartoon.newspaper.com) etc.

4. When you have added the addresses you wish to allow, click **Apply**.

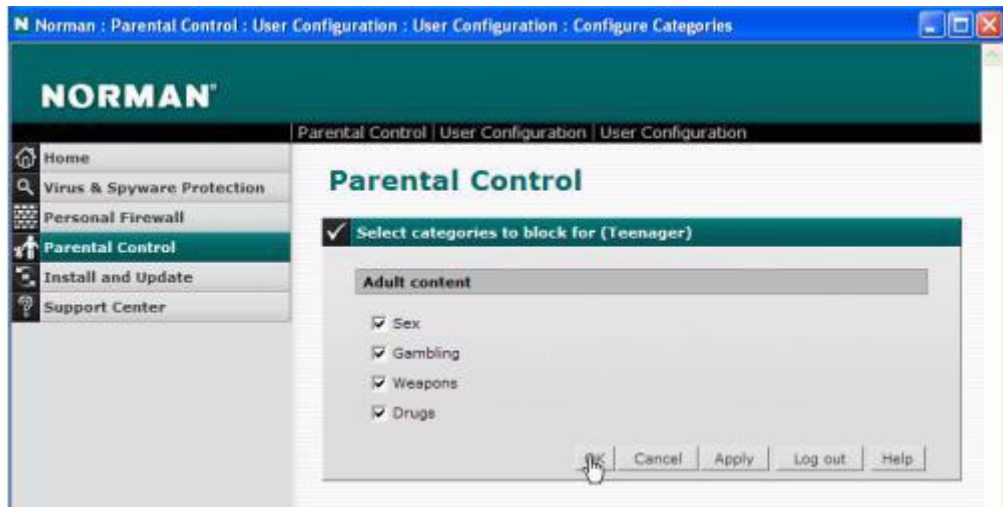
**Note:** The allowlist applies to *all* users in group *Child*.

## How to configure group Teenager

1. Select Parental Control | Group configuration | Teenager.
2. Click **Configure allowlist**. Type in web addresses in the format explained in step 3 above. Click **Apply** when you're done and then **OK** to return to the previous dialog.
3. Click **Configure blocklist** and type in the addresses you don't allow for users in the Teenager group. Note that you can activate/

deactivate both the allowlist and the blocklist by selecting/deselecting the option **Use blocklist**, alternatively **Use allowlist**.

4. Click **Apply** when you're done and then **OK** to return to the previous dialog.
5. Click **Select categories** and the following dialog appears:



6. By default all categories are selected, i.e. users in the group Teenager are denied access to web sites with content of this nature. If you decide to allow one or more categories, remove the checkmark for the relevant categorie(s). Click **Apply** to save possible changes.

## How to schedule Internet access

You have seen how you can control a user by assigning a group which restricts the surfing activity to approved web addresses. You can also restrict the time a user can spend on the Internet.

1. Go to Parental Control | User Configuration and click **Configure** for the user you want to schedule Internet access for.
2. Click **Select Internet Access**.
3. A calendar displaying the days of the week appears, without any restrictions. To block Internet access for a specific time, place the cursor on the desired day/time and left-click. Then move the cursor

to mark a period and left-click again. The selected field(s) are marked in red, denoting that this period is blocked for surfing. You can drag the cursor upwards/downwards or sideways right/left to extend the period you wish to block.

4. To edit blocked periods, place the cursor in a red field, click and drag the mouse over the area you wish to change.
5. When you are done configuring this user, click **Apply** to save your work.

# Support Center

If you need more assistance than the product documentation and online help can supply, you should go to the Support Center:



## Help and troubleshooting

Clicking the **Help and troubleshooting** link brings you to Norman's web, which offers a range of useful resources that in most cases will help you out. On this web site you'll find:

- Frequently Asked Questions (FAQ)
- technical knowledge base
- hot support topics
- Norman's Support Forum

- search facilities

If you cannot solve your problem with these tools, then try:

## Contact information

This page provides phone numbers and addresses so you can get in touch with your local Norman office/representative.

## Automatic repair

If you are experiencing any problems with your installed version of the Security Suite, you could always try to run an automatic repair before you contact support personnel.

When you click **Automatic repair**, a process is started in the background which checks your installation and if necessary updates files or components. You'll see the cog symbol in the tray menu while automatic repair is running. See 'Tray icons' on page 17 for an explanation of icons that affect the Security Suite.

If you don't have access to a graphical user interface, you can run `delnvc5.exe` from `c:\Program Files\Norman\nvc\bin` and choose the **Repair** option.

## Using eLogger to monitor your installation

eLogger is an application located in `...\norman\npm\bin` that keeps track on everything the Program Manager is doing in managing the Security Suite.

eLogger is always running if a working installation of the Security Suite is running. The application is collecting and storing the last 100 Kb of information on Security Suite-related activities.

You can save eLogger information which automatically is stored as txt files in `...\Norman\logs` with the name `ELG_mmdd_hhmmss`.

There is no need to worry even if there are numerous entries in the log. The eLogger records everything that's related to the Security Suite, so many entries don't suggest that something is wrong.

eLogger information can be particularly useful for support personnel.



## Uninstalling the Security Suite

You can uninstall the product using Windows' Control Panel's **Add/Remove programs** (on Vista, from Programs and Features), or running `delnvc5.exe` from `c:\Program Files\Norman\nvc\bin` and choose the **Remove** option. When the program is removed, restart the computer.

# Appendix A

## What is a sandbox?

Sandbox is the term that best describes the technique that is used to check if a file is infected by an unknown virus. The name is not randomly picked, because the method allows untrusted, possible viral code to play around on the computer – not in the real computer, but in a simulated and restricted area within the computer. The sandbox is equipped with everything a virus expects to find in a real computer. This is a playground where it is safe to let a virus replicate, but where every step is carefully monitored and logged. The virus is exposing itself in the sandbox, and because its actions have been recorded, the cure for this new perpetrator can be generated automatically.

Today, a new email worm can infect ten thousands of workstations in a matter of seconds. Norman's sandbox functionality can prove to be a valuable tool for trapping new destructive code.